Institut français
des sciences et technologies
des transports, de l'aménagement
et des réseaux

Améliorer la connaissance et le fonctionnement du réseau

Emmanuel.Reuter@ifsttar.fr

IFSTTAR

Plan

- PSSIE
  - **Cadre général**
- Politique Réseau
  - Utilisateurs
  - Machines
- Interconnexion
  - RENATER, Celeste, etc..
- Réseaux Locaux
  - Contrôle d'accès
  - SubVlans
  - DHCP Snooping
  - Logs
- Cartographie
  - IMC, Cacti, Développement interne
  - Métrologie

Politique de Sécurité des Systèmes d'information de l'état

- **Gestion des réseaux**
  - Cloisonnement du réseau de la structure
    - Selon les types d'utilisation
    - Selon le niveau de sécurité
  - Procédure d'enregistrement et d'analyse à posteriori des logs

- **Gestion des contrats de sous-traitance SI**
  - Encadrement contractuel des accès au réseau
    - Volet sécurité avec l'opérateur d'interconnexion
- **Organisation**
  - Analyse des risques dans le SI ?
    - Groupe de travail qui rédige les clauses contractuelles pour les contrats
  - Engagement de la DSI pour diminuer les risques
    - Questionnaire du ministère et évaluation de l'avancement de la PSSIE (/an)
    - On s'engage à appliquer la PSSIE et la surveiller au quotidien

PSSIE : « On fait quoi »

- Structure existante
  - Etat des lieux
    - Bases de données, sites web, matériels actifs, etc
  - Recensement des mesures en place
  - Inventaire des documents existants
  - Mesures déjà appliquées
- Puis vers où on va évoluer
  - Regrouper les documentations au même endroit
  - Technique de nommage « réseaux »
    - Bâtiment, étage, baie, position GPS, etc..
    - Nommage des règles pour les firewalls
  - Ticketing, liste de diffusions, etc..
    - Glpi, incident sécurité

Plan

- PSSIE
  - Cadre général
- Politique Réseau
  - **Utilisateurs**
  - **Machines**
- **Interconnexion**
  - RENATER, Celeste, etc..
- Réseaux Locaux
  - Contrôle d'accès
  - SubVlans
  - DHCP Snooping
  - Logs
- **Cartographie**
  - IMC, Cacti, Développement interne
  - Métrologie

Ordinateurs nomades

- Postes nomades antivirus et pare-feu local
  - Postes validés par la DSI, le VPN officiel,
  - Poste dans l'AD, pour le télétravail
- Blocage des ordinateurs portables
  - Problématique des adaptateurs USB/Ethernet
    - Problématique de la station d'accueil
    - Adresse MAC du bios de la machine

Garantir que c'est une machine IFSTTAR

Ordinateurs nomades

- Solution(s)
  - Utilisation de la RJ45 du portable (PC)
    - Non déclaration de la station d'accueil
    - Agent sur les postes
  - Utilisation de la carte Wifi des Macs (Apple) portables pour connaître la machine
- Tablettes et portables
  - Avec adaptateur RJ 45
  - Déclaré dans l'AD si possible
- Sinon Autres gammes
  - Toutes connectées via le WIFI via EDUROAM, aucune interaction directe avec le réseau IFSTTAR

Plan

- PSSIE
  - Cadre général
- Politique Réseau
  - Utilisateurs
  - Machines
- **Interconnexion**
  - **RENATER, Celeste, etc..**
- Réseaux Locaux
  - Contrôle d'accès
  - SubVlans
  - DHCP Snooping
  - Logs
- **Cartographie**
  - IMC, Cacti, Développement interne
  - Métrologie

Interconnexions avec les autres organismes ou de tutelles

- RIE (ligne physique modem)
- RENATER (sortie Internet Cisco)
  - Filtrage des flux entrant et sortant par le palo-alto (Filtrage+IPS/IDS), Acls (Cisco), etc..
- CELESTE
  - Pour l'interconnexion des sites sans filtrage
  - Rempli les conditions de la PSSIE (chiffrement)

Interconnexions avec les autres organismes ou de tutelles

- Autres organismes
  - Cloisonnement des ressources en cas de partage de locaux
    - Vlan avec sortie contrôlé, chiffrement si passage sur notre réseau officiel, sub-vlans
    - VPN IpSec pour connexion vers les partenaires
    - Filtrage des accès vers les serveurs locaux via des parefeux
    - Exemple :
      - Vlans privés/différents (Cerema, ENPC) sur le même campus
      - Chiffrement par DHCP+proxy+VPN (A éviter de faire en urgence…. …)

Nécessité de prévoir une procédure

Sécurité des réseaux nationaux

- Systèmes autorisés sur le réseau
  - Que les matériels maitrisés par la DSI
  - Pour les autres des interactions limitées (mail, web, calcul, très restreints, accès filtrés)
  - Accès VPN vers l'IFSTTAR
    - Nomades vers le firewall « Fortigate »
    - Surtout pour le télétravail
- Protection des informations
  - Accès Internet passe par le même point de sortie
    - Filtrage par pare-feu et ACLs
  - Spécifiquement via des serveurs Proxy
    - (wpad utilisé)

Passage via le proxy

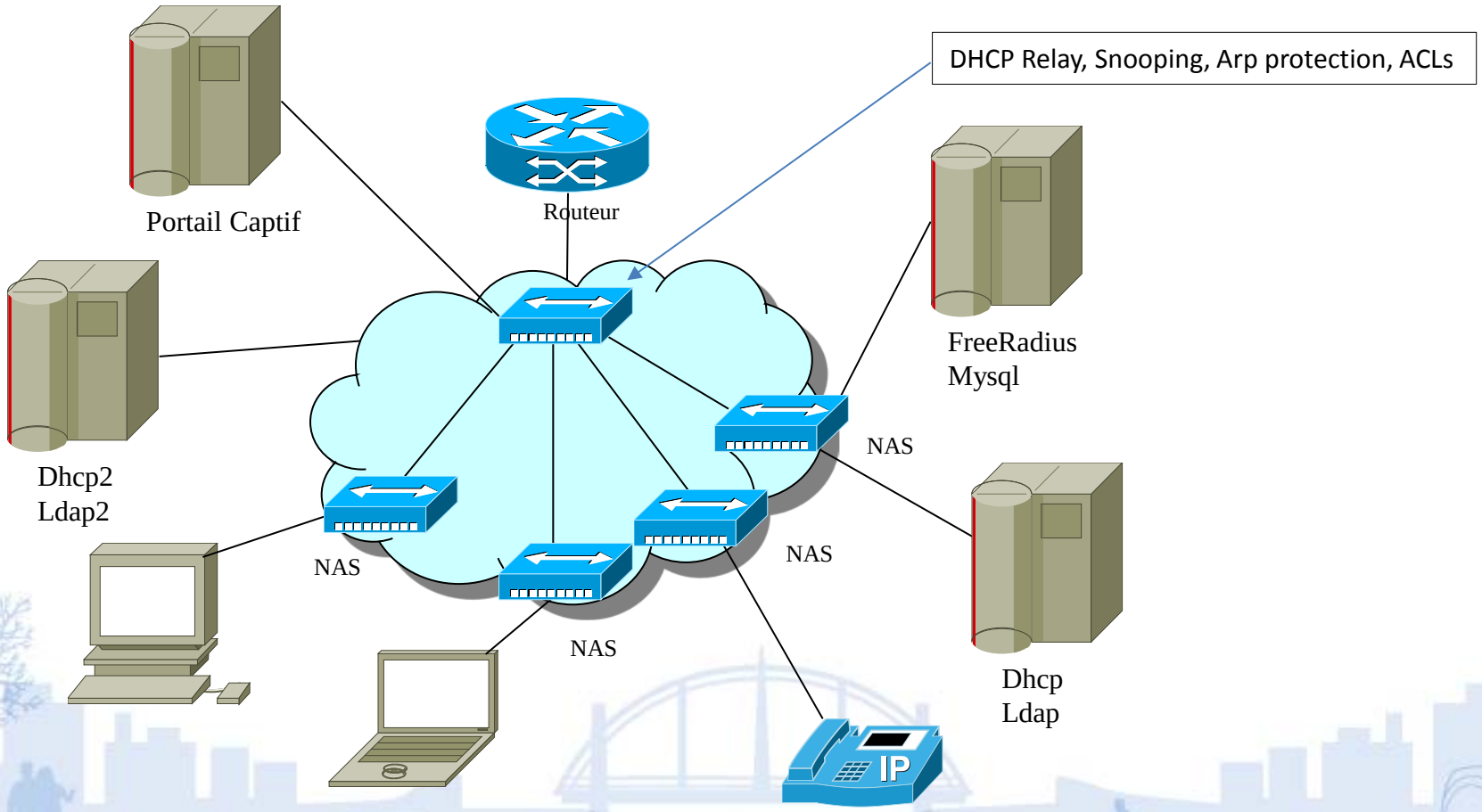
- Pour faciliter la gestion des configurations
  - Toutes les connexions extérieures via le Proxy
  - Le client cherche wpad.domaine.fr, fournit par le DHCP (option 252)
  - Charge ensuite http://wpad.domaine.fr/wpad.dat,

```
function FindProxyForURL(url, host)
        {
            if (dnsDomainIs( host,"euro-access.org")) return "DIRECT";
            if (isInNet(host, "127.0.0.1", "255.255.255.255")) return "DIRECT";
            if (isInNet(host, "x.y.0.0", "255.255.0.0")) return "DIRECT";
            if (dnsDomainIs( host,"eu-admin.net")) return "PROXY
x.y.145.122:3128";
            if (isPlainHostName(host)) return "DIRECT";
            if (url.substring(0, 4) == "ftp:") return "DIRECT";
            if (url.substring(0, 6) == "https:") return "DIRECT";
            return  "PROXY x.y.18.26:3128";
        }
```

Plan

- PSSIE
  - Cadre général
- Politique Réseau
  - Utilisateurs
  - Machines
- Interconnexion
  - RENATER, Celeste, etc..
- **Réseaux Locaux**
  - **Contrôle d'accès**
  - **SubVlans**
  - **DHCP Snooping**
  - **Logs**
- Cartographie
  - IMC, Cacti, Développement interne
  - Métrologie

Contrôle d'accès au réseau filaire : NAC



NAC: Contrôle d'accès

- Début du déploiement en 2008
- Basée sur un LDAP central
  - 1 à 2 réplicas par site
- Tout fonctionne ensuite sur le LDAP
  - Un serveur DHCP (voire 2) par site qui lit dans le LDAP
  - Tout le réseau est configuré de la même manière
    - Fixe ou migrant
  - Une seule déclaration des adresses MAC dans le LDAP
  - N'importe quelle machine de l'IFSTTAR peut se connecter n'importe où
    - Mobilité filaire
    - Machine configurée accède en – d'une minute au réseau
  - Mysql pour l'accounting

Solution NAC : LDAP

- Structure du LDAP
  - dhcpStatements: fixed-address 192.168.182.193
  - objectClass: dhcpHost
  - objectClass: dhcpOptions
  - objectClass: ieee802Device
  - objectClass: radiusprofile
  - dhcpOption: broadcast-address 192.168.182.255
  - dhcpOption: routers 192.168.182.201
  - dhcpOption: subnet-mask 255.255.255.0
  - dhcpHWAddress: ethernet 00:0b:8*:**:**:**
  - macAddress: 00:0b:8*:**:**:**
  - uid: 000b8*******
  - radiusTunnelPrivateGroupId: 182
  - radiusTunnelType: VLAN
  - radiusTunnelMediumType: IEEE-802

Config sur HPE : Nac

- Sur H3C
- # Autorisation de la ToIP
  - voice vlan mac-address 0008-5d00-0000 mask ffff-ff00-0000 description TEL-ASTRA
- # Config interface
  - interface Ethernet1/0/5
  - port link-mode bridge
  - port link-type trunk
  - port trunk permit vlan 1 9 16 to 19 1891 193 1054
  - undo voice vlan mode auto
  - voice vlan 19 enable
  - stp edged-port enable
  - mac-authentication
  - mac-authentication guest-vlan 1
  - mac-authentication critical vlan 189
  - mac-authentication domain bron.auth

Contrôle d'accès : interface

NASIPAddress	Port	Adresse Ethernet
192.192.56.101	4	00:20:xx:yy:zz:hh

Reseau	Ethernet	Nom	Derniere connexion	Switch (Port)
192.168.16.10	0024exxxx	-portable_dbr	N/A	
192.168.16.11	8cdcyyyyd654c	-P002	2017-10-24 15:06:00	192.192.56.106(23)
192.168.16.12	c8xxyy78342c	-P-013	2017-09-14 09:34:55	192.192.56.202(1)
192.168.16.13	0025yxxyhh15	-Bou_Mac2	N/A	
192.168.16.15	c81f66xyyxxy	-DA-15452	N/A	
192.168.16.16	002564715930	-Joyeux_Luron	N/A	
192.168.16.17	180xxyyxx42f	-Decolle_1	2017-09-06 09:11:41	192.192.56.202(1)
192.168.16.18	3c970ehhxxyy	-Portable	N/A	

Sécurité des réseaux locaux : sub-vlans

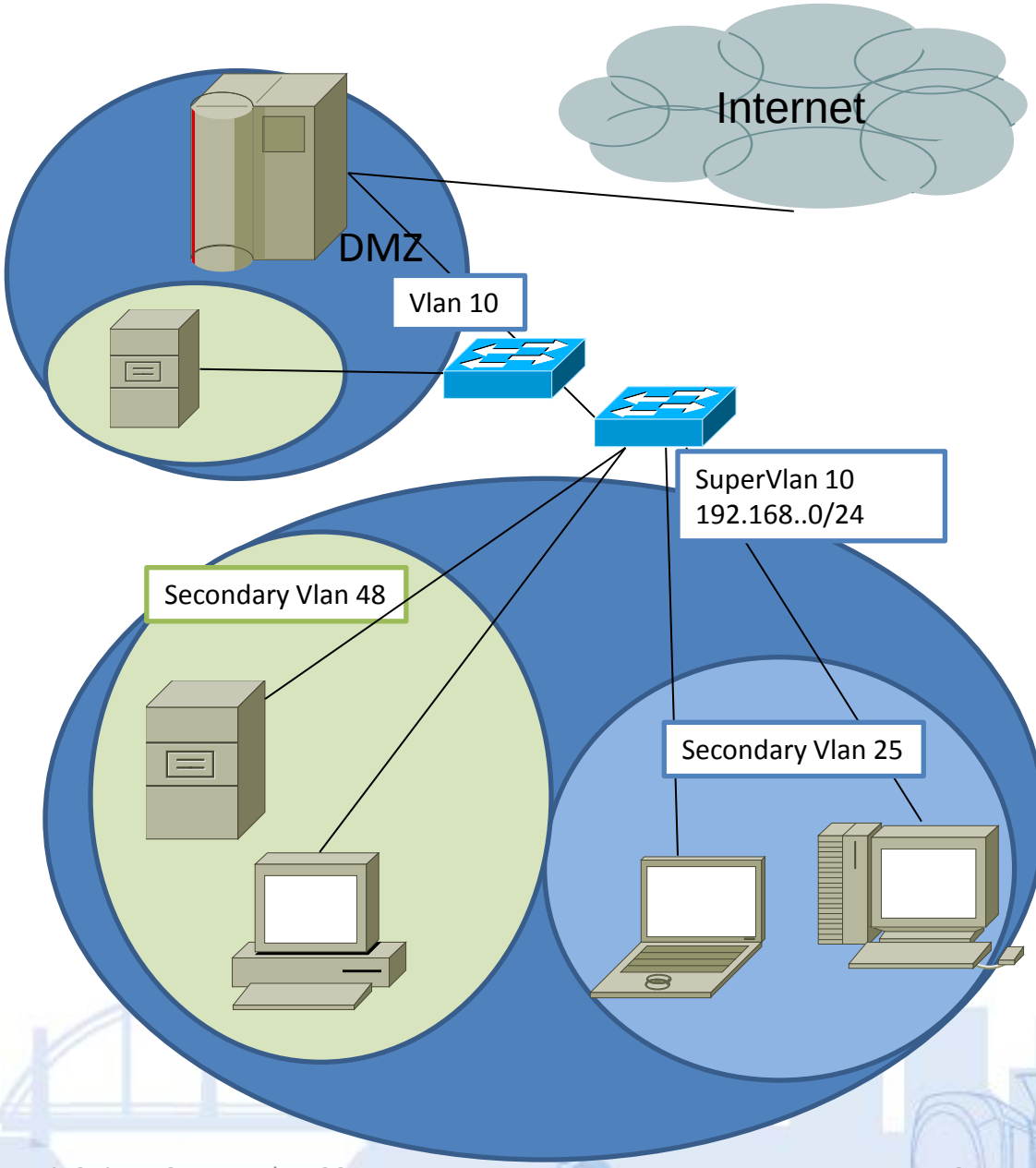
- Vlan traditionnel
  - Toutes les machines sont accessibles dans le VLAN.
  - Trop simple, on complique
- Eviter de créer un VLAN à chaque fois qu'une machine doit être protégée
  - Problématique de gestion des IPv4 (RFC 3069)
  - Interdire à des machines du même switch et de même VLAN de communiquer entre elles
    - Protection utilisée dans les hôtels en connexion filaire
    - Identique à la protection des clients WIFI sur hotSpot
- Primary Vlan (RFC 5517)
  - Un seul domaine de Broadcast
  - On « encapsule » des Vlans dans des Vlans
    - Pas de découpage à gogo des plages IP v4

Sécurité des réseaux locaux : sub-vlans (suite)

- Port « Isolated »
  - Utilisé pour une machine devant avoir accès à un nombre limité d'interfaces de sortie
- Community Port
  - Groupe de ports privés pouvant communiquer entre eux directement, et avec le port Promiscuous
- Port Promiscuous (Primary Vlan)
  - Peut communiquer avec les machines des sub-vlans
  - Plusieurs ports peuvent être configurés dans le primary vlan
  - La cascade réseau (uplink) est un port Promiscuous

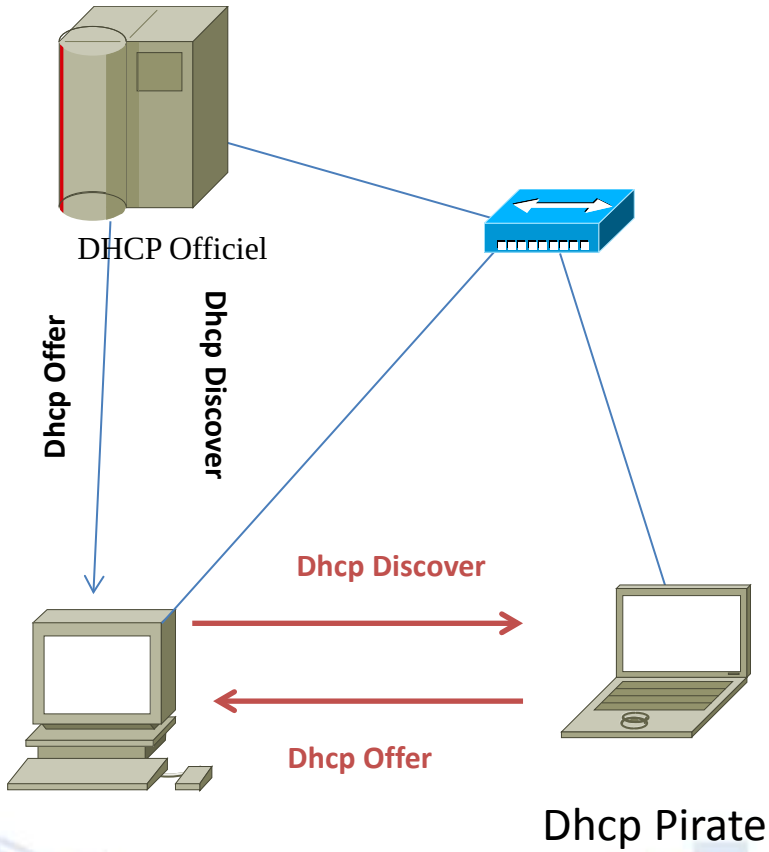
Exemple

- Les machines du subvlan 48 communiquent entre elles
- Les machines du subvlan 25 communiquent entre elles
- Les machines des deux sub-vlans ne se voient pas.
- Les deux vlans sont englobés dans le Vlan 10, qui lui a une interface IP
- Elles peuvent communiquer uniquement via le SuperVlan10 (proxy-arp)



Sécurisation des protocoles réseaux : DHCP

- Mécanisme de protection des couches basses
  - DHCP Snooping, arp-protection (tous réseaux confondus)
- Objectif
  - Eviter d'autres serveurs DHCP non officiels
  - Eviter les perturbations réseaux
  - Eviter les utilisations des adresses MAC officielles



Pollution du DHCP

- On passe au DHCP-Snooping et ARP-Protection
- Config cœur de réseau

- dhcp relay server-group 2 ip 192.168.201.232
- dhcp relay server-group 3 ip 192.168.210.2
- dhcp relay server-detect

- interface Vlan-interface192
- ip address 192.168.192.254 255.255.255.0
- dhcp select relay
- dhcp relay server-select 2
- proxy-arp enable
- udp-helper server 192.168.201.232

- #
- # Pour faire du WDS à l'IFSTTAR
- interface Vlan-interface195
- ip address 192.168.195.254 255.255.255.0
- dhcp select relay
- proxy-arp enable
- dhcp relay server-select 3

- Switch client autre que le cœur –Procurve)
- Une définition par VLAN, car une IP par Vlans sur le cœur

- dhcp-snooping
- dhcp-snooping authorized-server 192.168.192.254
- dhcp-snooping authorized-server 192.168.195.254
- dhcp-snooping option 82 untrusted-policy keep
- no dhcp-snooping verify mac
- dhcp-snooping vlan 1-1103 1105-1970 1972-4093

Avantage : Si un server DHCP pirate se monte, il ne répondra jamais car les packets sont droppés/interceptés

Sécurisation des matériels et protocoles réseaux

- Annonce de routage
  - Routage statique inter-sites
- Sur les routeurs
  - Désactivation des interfaces inutiles sur les routeurs
  - Services inutiles
- Authentification par défaut
  - Changement de toutes les communautés SNMP public/private du réseau
  - Accès filtré par IP de management

Synchronisation des logs et horloges

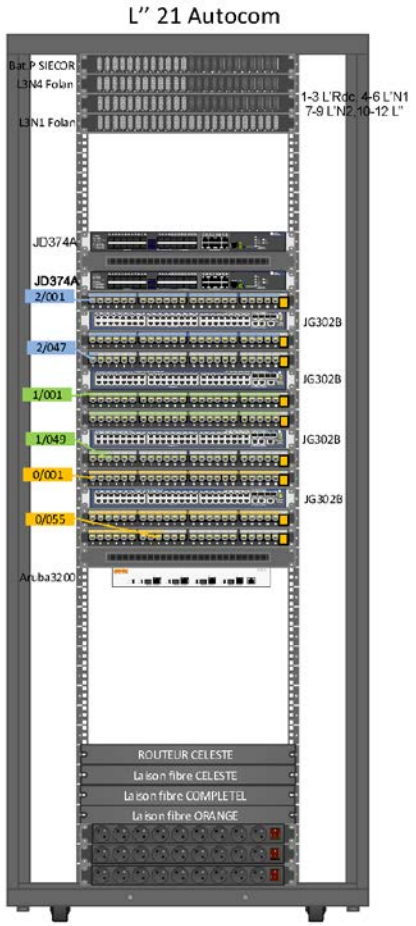
- Analyse des logs (journaux informatiques)
  - Retracer la chronologie d'un événement
  - Logs centralisés sur un serveur
  - Configuré sur
    - serveurs,
    - routeurs,
    - PC utilisateurs si nécessaire
  - Logguer mais pas tout
    - Des flux applicatifs
    - Des flux d'administration du réseau
- Notamment en multi-sites
  - Trace des incidents…

Plan

- PSSIE
  - Cadre général
- Politique Réseau
  - Utilisateurs
  - Machines
- Interconnexion
  - RENATER, Celeste, etc..
- Réseaux Locaux
  - Contrôle d'accès
  - SubVlans
  - DHCP Snooping
  - Logs
- **Cartographie**
  - **IMC, Cacti, Développement interne**
  - **Métrologie**

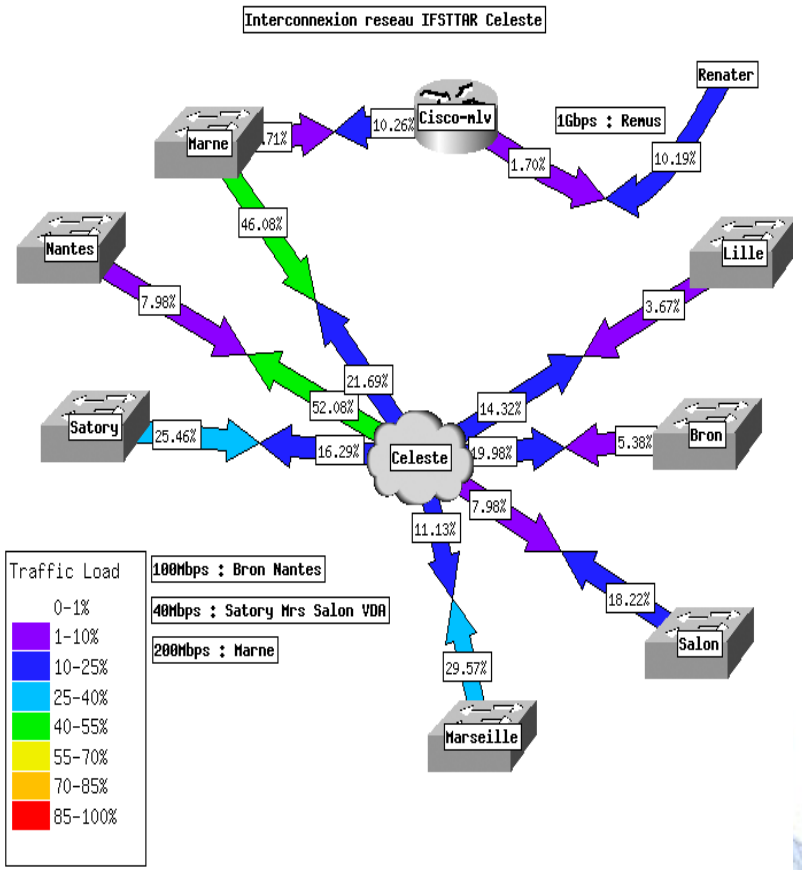
Cartographie des bâtiments

- Beaucoup de documentation
  - Chaque port de switch est associé avec le numéro d'une prise
    - Intérêt pour le suivi des demandes de travaux
    - Seules les prises actives sont brassées
    - Beaucoup de travail si on doit rebrasser une prise
      - Nécessité de la documentation et d'une procédure !!
- Utilisation de visio pour schématiser les baies réseaux



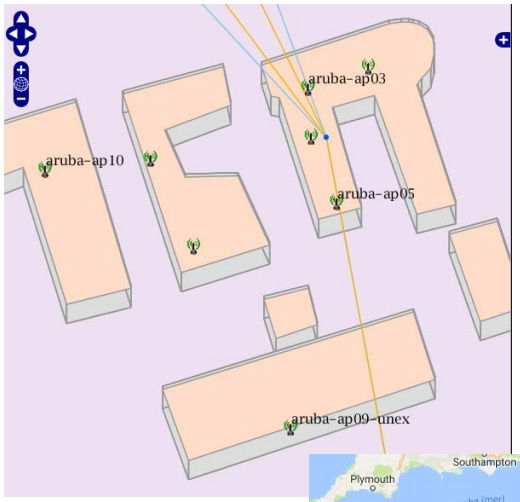
Cartographie et indicateurs du réseau

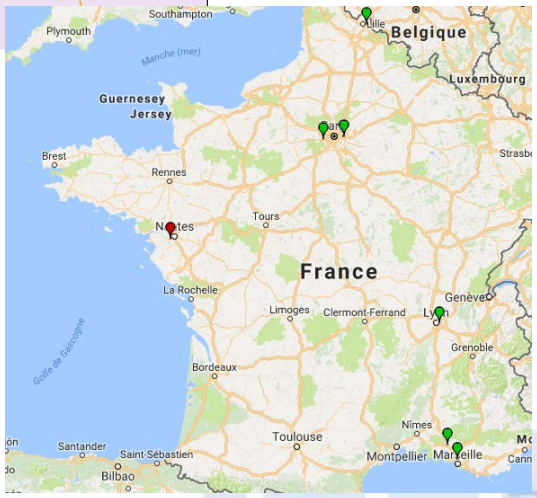
- Maintenir une base de données des matériels
  - Cacti
  - Pouvoir écrire des scripts
  - Suivre rapidement les IOS de chaque matériels
  - Extraire des données pour faire des indicateurs



Cartographie et documentation du réseau

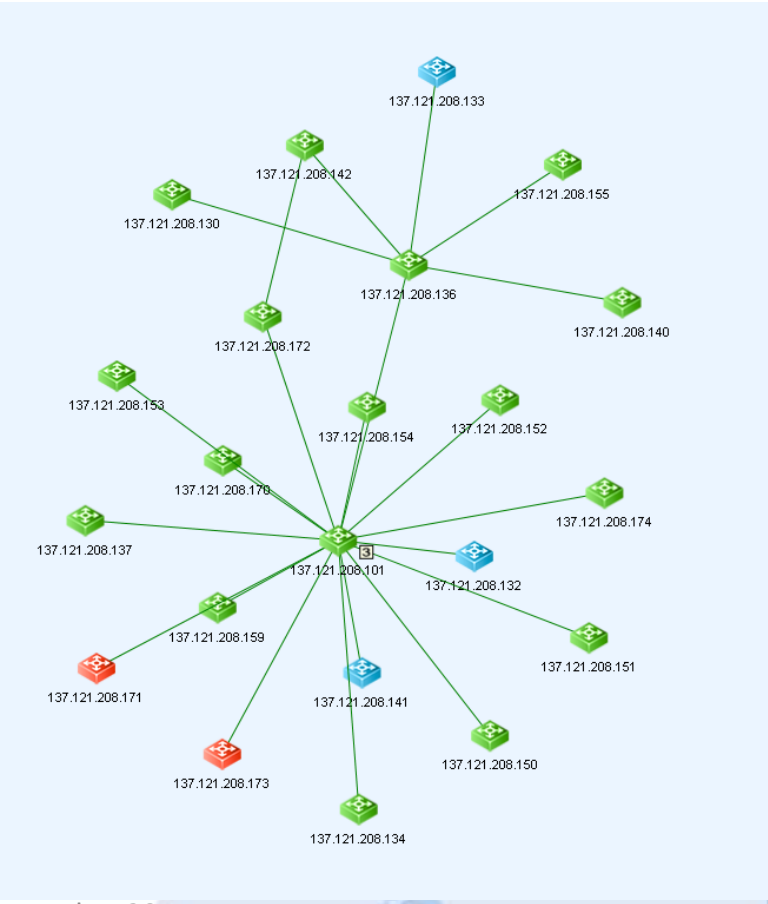
- Via des données géoréférencées avec positionnement des baies réseaux, des serveurs, des bornes Wifi..
- Module GPSMap dans Cacti (alertes notamment)





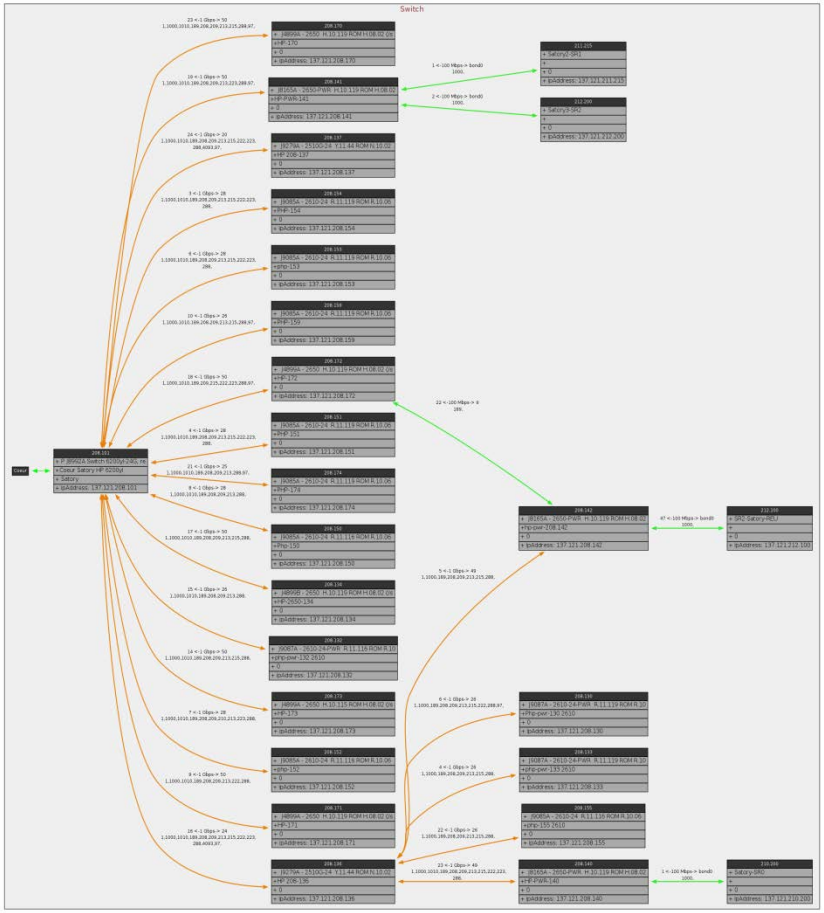
Cartographie et documentation du réseau

- Maintenir à jour la cartographie du réseau
  - Soit IMC



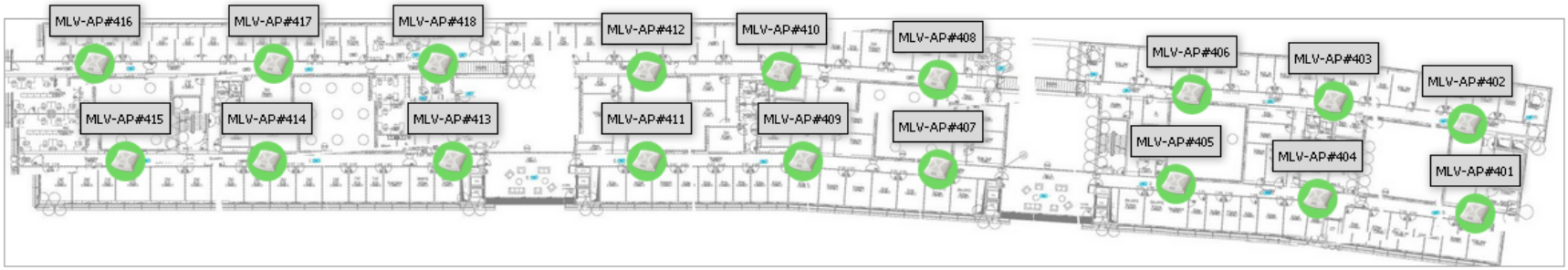
Cartographie et documentation du réseau

- Soit via Cacti + développement
  - LLDP pour une construction automatique des schémas de réseau
    - Débit du lien en couleur
    - Vlans affectés
    - Position des machines, bornes Wifi, serveurs Virtuels, etc..



Cartographie Wifi

- ARUBA
- Position des bornes WIFI
  - Nécessité d'avoir les plans à intégrer dans l'outil
  - Position des utilisateurs



Cartographie et documentation du réseau

- Tenir à jour des documentations sur le réseau
  - Sauvegarde des configurations (IMC)
  - Cron :
    - Tftp pour backup des configurations Cisco, HPE, HPN, en plus
      - Configuration en SNMP et upload en tftp

Récupération des configs Cisco

- Cisco
- #
- snmpset -v 2c -c $COMMUNITY $HOSTNAME 1.3.6.1.4.1.11.2.14.11.5.1.7.1.5.6.0 i 2
- touch $FILENAME
- chmod 777 $FILENAME

- tftp $HOSTNAME <<!
- timeout 1
- get running-config $FILENAME
- quit
- !
- #mv running-config $FILENAME
- #
- # a this point, lock tftp access
- #
- snmpset -v 2c -c $COMMUNITY $HOSTNAME 1.3.6.1.4.1.11.2.14.11.5.1.7.1.5.6.0 i 1

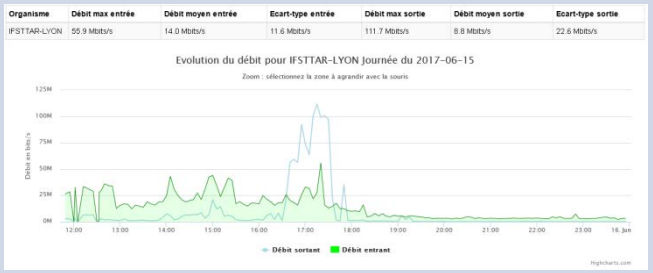
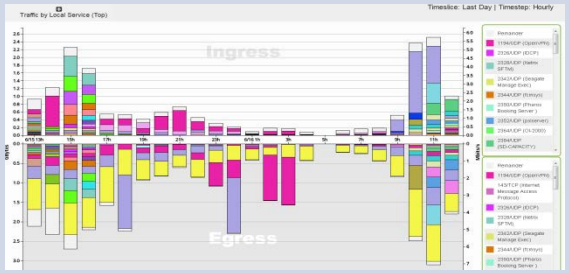
Récupération des configs HPE

- H3C
- # Normally, have to get a empty row and destroy it after completion
- # Destroy row
- #
- snmpset -v 2c -c $COMMUNITY $HOSTNAME 1.3.6.1.4.1.25506.2.4.1.2.4.1.9.2 i 6
- # hh3cCfgOperateRowStatus (9) - hh3cCfgOperateFileName (4)- hh3cCfgOperaServerAddress (5)
- snmpset -v 2c -c $COMMUNITY $HOSTNAME 1.3.6.1.4.1.25506.2.4.1.2.4.1.2.2 i 3 1.3.6.1.4.1.25506.2.4.1.2.4.1.3.2 i 2 1.3.6.1.4.1.25506.2.4.1.2.4.1.4.2 s $FILENAME 1.3.6.1.4.1.25506.2.4.1.2.4.1.5.2 a $TFTPSERVER 1.3.6.1.4.1.25506.2.4.1.2.4.1.9.2 i 4
- #
- # gets the result command
- echo
- echo "##"
- echo "Getting result of SNMP Command"
- echo "##"
- echo

- snmpwalk -v 2c -c $COMMUNITY $HOSTNAME 1.3.6.1.4.1.25506.2.4.1.2.5.1

Métrologie

- Surveillance des flux en entrée et en sortie

NetMET v2 pour la métrologie longue durée	Znets pour du quasi temps-réel
	

Merci de votre attention

Questions ?

Non, vous êtes bons ;-)

Ifsttar
14-20 Bld. Newton - Cité Descartes
Champs sur Marne
77447 Marne-la-Vallée Cedex 2 - France
www.ifsttar.fr